AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
One (1) Twitter account, hosted at premises controlled by Twitter, Inc., located at 1355 Market Street, Suite 900, San Francisco, CA, more fully described in Attachment A-1

Case No. MJ19-359

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

One (1) Twitter account, hosted at premises controlled by Twitter, Inc., located at 1355 Market Street, Suite 900, San Francisco, CA, more fully described in Attachment A-1, incorporated herein by reference

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1 for a list of information to be disclosed, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1028A; 1028(a)(7);	Aggravated Identity Theft; Identity Theft;
18 U.S.C. § 1029(a)(2); 1030;	Access Device Fraud; Computer Fraud;
18 U.S.C. § 1343	Wire Fraud

The application is based on these facts:

✓ See Affidavit of Joel Martini, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or ☐ telephonically recorded.

Joel Martini

Applicant's signature

Joel Martini, Special Agent FBI

Printed name and title

◉ The foregoing affidavit was sworn to before me and signed in my presence, or
○ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 07/30/2019

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

USAO: 2019R00675

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Joel Martini, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since January 2017. I am assigned to the Cyber Squad, where I investigate computer intrusions and other cybercrimes. I have received training, and gained experience in, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, cybercrimes, computer evidence identification, computer evidence seizure and processing, and criminal law and procedures. I have received advanced training in the acquisition and analysis of digital evidence (both network and host-based) responding to computer intrusions and other incidents. I have participated personally in the execution of search warrants involving the search and seizure of computer equipment.

2. Prior to my employment as a Special Agent, I received a Bachelor of Science in Information Systems from Corban University. I also subsequently worked as a Computer Forensic Examiner for the FBI for approximately five years. During the course of that employment, I became familiar with the design and operation of various electronic devices, networks, and websites, including the technology described herein.

3. I currently am conducting an investigation of Paige Adele Thompson, also known by the alias "erratic," for intruding into servers rented or contracted by Capital One Financial Corporation ("Capital One"), a financial services company, from Amazon.com, Inc., also doing business as Amazon Web Services (AWS) ("Amazon"), a company that provides cloud computing services, and for exfiltrating and stealing information, including credit card applications and other documents, from Capital One.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (collectively, "**SUBJECT ACCOUNTS**") that are stored at premises controlled by an electronic communications service and/or remote computer service provider ("Provider"), referenced below. The information to be searched is described in the following paragraphs and in Attachments A, which are incorporated herein. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the following:

a. **Twitter, Inc.** ("Twitter"), located at 1355 Market Street, Suite 900, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-1, pertaining to the following account(s), identified in Attachment A-1: **@0xA3A97B6C, with username "ERRATIC" ("SUBJECT ACCOUNT 1");**

b. **Slack Technologies** ("Slack"), located at 500 Howard Street, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-2, pertaining to the following account(s), identified in Attachment A-2: **netcrave.slack.com ("SUBJECT ACCOUNT 2");**

c. **GitHub, Inc.** ("GitHub"), located at 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-3, pertaining to the following account(s), identified in Attachment A-3: **https://gist.github.com/paigeadelethompson/ ("SUBJECT ACCOUNT 3").**

Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B. This warrant is requested in connection with an on-going investigation in this district by the Seattle Field Office of the Federal Bureau of Investigation (FBI).

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), have been committed by Paige Thompson, as described below, as well as perhaps other unknown persons. There is also probable cause to search the information described in Attachments A for evidence, instrumentalities, contraband or fruits of these crimes, as described in Attachments B.

6. The facts set forth in this Affidavit are based on my own personal knowledge, including interviews I have conducted and my review of documents related to this investigation; information obtained from other individuals, including other law enforcement officers and investigators and employees of Capital One; and my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation, but rather those relevant to the determination of whether probable cause exists to issue the requested search warrant.

SUMMARY OF PROBABLE CAUSE

7. The FBI is conducting an investigation into a network intrusion into servers rented or contracted by Capital One from Amazon. Capital One is a financial services company that, among other things, issues credit cards. The evidence in this case shows that Thompson, who resides at 6520 28th Avenue South, Seattle, Washington (the "SUBJECT RESIDENCE"), is the person who committed this intrusion.

8. Evidence linking Thompson to the intrusion includes the fact that information obtained from the intrusion has been posted on a GitHub page that includes Thompson's full name – paigeadelethompson – as part of its digital address (namely, **https://gist.github.com/paigeadelethompson/ (SUBJECT ACCOUNT 3)**), and that is linked to other pages that belong to Thompson and contain her resume. In addition, records obtained from Capital One indicate that Internet Protocol addresses used by the intruder are controlled by a company that provides virtual private network services and that was used by Thompson to make postings on the internet service GitHub, including very close in time to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

intrusions. Moreover, Thompson also has made statements on social media fora evidencing the fact that she has information of Capital One, and that she recognizes that she has acted illegally.

TERMS AND DEFINITIONS

9. For the purpose of this affidavit, I use the following terms as described below:

a. A server is a computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called clients. Servers can be physically located anywhere with a network connection that may be reached by the clients. For example, it is not uncommon for a server to be located hundreds (or even thousands) of miles away from client computers. A server may be either a physical or virtual machine. A physical server is a piece of computer hardware configured as a server with its own power source, central processing unit or units, and associated software. A virtual server typically is one of many servers that operate on a single physical server. Each virtual server shares the hardware resources of the physical server, but the data residing on each virtual server is segregated from the data on other virtual servers on the same physical machine.

b. An Internet Protocol address (an "IP address") is a unique numeric address used by devices, such as computers, on the internet. Every device attached to the internet is assigned an IP address, so that internet traffic sent from, and directed to, that device may be directed properly from its source to its destination. Most internet service providers control a range of IP addresses. Generally, a static IP address is permanently assigned to a specific location or device, while a dynamic IP address is temporary and periodically changes.

c. The Onion Router (or "TOR") is an anonymity tool used by individuals to conceal their identities, including the origin of their internet connection, that is, their IP addresses. TOR bounces communications through several intermediate computers (relays), each of which utilizes encryption, thus anonymizing the IP address of the computer of the individual using TOR.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. A virtual private network (a "VPN") is a secure connection over a less secure network, such as the internet. A VPN uses shared public infrastructure, but maintains privacy through security procedures and tunneling protocols. It encrypts data at the sending end, decrypts it at the receiving end, and sends the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. A VPN also may encrypt the originating and receiving network addresses.

10. Throughout this Affidavit, I also refer to a number of companies and to services that they offer:

a. GitHub is a company that provides webhosting and allows users to manage and store revisions of projects. Although used mostly for software development projects, GitHub also allows users to manage other types of files.

b. IPredator is a company that offers prepaid VPN service to customers, using servers based in Sweden.

c. Meetup is an Internet-based platform designed to let people find and build local communities, called "groups."

d. Slack is a cloud-based set of team-collaboration software tools and online services. Slack allows users to establish "channels," in which a team can share messages, tools, and files.

e. Twitter is company that operates a social networking site that allows users to establish accounts, post short messages, and receive other users' messages.

THE INVESTIGATION

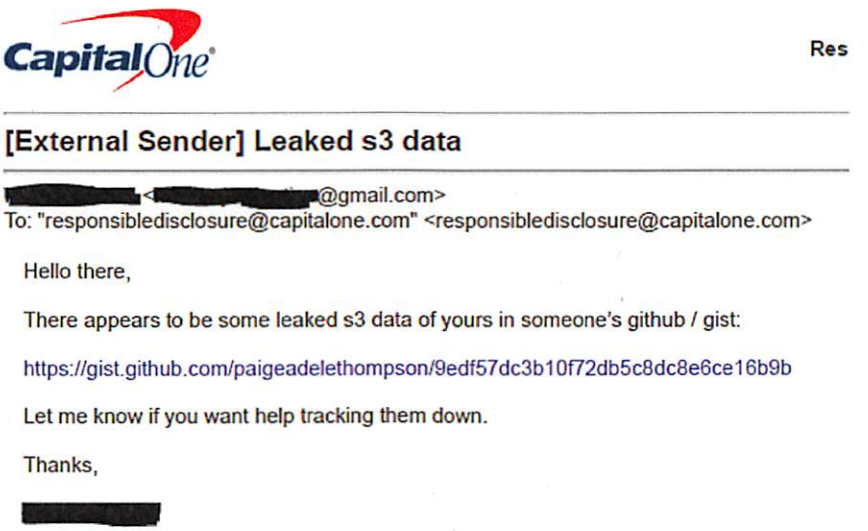
A. The Intrusion and Exfiltration

11. Capital One is a financial services company that offers, among other products, credit cards. Capital One maintains an e-mail address through which it solicits disclosures of actual or potential vulnerabilities in its computer systems, so that Capital One can learn of, and attempt to avert, breaches of its systems. Among others who send e-mails to this address are individuals who sometimes are called "ethical" or "white hat" hackers. Like other

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

companies, Capital One often will make payments to individuals who provide information concerning actual or potential vulnerabilities.

12. On July 17, 2019, an individual – who previously was unknown to Capital One - emailed this e-mail address. The individual's e-mail stated that there appeared to be leaked data belonging to Capital One on GitHub, and provided the address of the GitHub file containing this leaked data, which was associated with **https://gist.github.com/paigeadelethompson/ (SUBJECT ACCOUNT 3)**. The precise address provided for this file was https://gist.github.com/paigeadelethompson/*****. [Throughout this affidavit, I use ***** to substitute for other characters, often more than five characters.]



Res

[External Sender] Leaked s3 data

[redacted]<[redacted]@gmail.com>
To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com/paigeadelethompson/9edf57dc3b10f72db5c8dc8e6ce16b9b

Let me know if you want help tracking them down.

Thanks,

[redacted]

Significantly, this address includes the name paigeadelethompson, which I know to be Thompson's full name. The individual providing this information offered to help track down the person who had posted this information. Further, in subsequent communications with Captial One representatives, the individual provided additional information related to the alleged data theft, including additional files associated with **SUBJECT ACCOUNT 3**:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

---------- Forwarded message ---------
From: [redacted] <[redacted]@gmail.com>
Date: Fri, Jul 19, 2019 at 1:53 PM
Subject: Re: [External Sender] Leaked s3 data
To: Kathryn [redacted] <[redacted]@capitalone.com>
CC: [redacted] <[redacted]@[redacted].com>

Hey Kathryn,

Thanks for speaking yesterday. I'm attaching the links as well as screenshots to this Twitter DM where this person drops the following gist links:

(in order) --

https://gist.github.com/paigeadelethompson/1d046e22a54995ebf82040d9279317cc

https://gist.github.com/paigeadelethompson/9edf57dc3b10f72db5c8dc8e6ce16b9b

https://gist.github.com/paigeadelethompson/b8cc49efffb2949857ccc60d3e3d8fa3

https://gist.github.com/paigeadelethompson/3bbb3f7fc187f83264455f51ce18525e

Please let me know if there is anything I can clarify. =)

Thanks and kind regards,

[redacted]

Further, the individual identified and sent screenshots of direct messages with the user of a Twitter user, namely, **@0xA3A97B6C, with username "ERRATIC" (SUBJECT ACCOUNT 1)**, associated with the same actor. The individual providing the information also subsequently has indicated that he/she hopes to be paid for providing the information.

13. After receiving this information, Capital One examined the GitHub file posted on **SUBJECT ACCOUNT 3**,, which was timestamped April 21, 2019 (the "April 21 File"). Capital One determined that the April 21 File contained the IP address for a specific server. A firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data in Capital One's storage space at the Cloud Computing Company.

14. Capital One determined that the April 21 File contained code for three commands, as well as a list of more than 700 folders or buckets of data.

- Capital One determined that the first command, when executed, obtained security credentials for an account known as ISRM-WAF-Role that, in turn, enabled access to certain of Capital One's folders at Amazon.
- Capital One determined that the second command (the "List Buckets Command"), when executed, used the ISRM-WAF-Role account to list the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

names of folders or buckets of data in Capital One's storage space at Amazon.

- Capital One determined that the third command (the "Sync Command"), when executed, used the ISRM-WAF-Role to extract or copy data from those folders or buckets in Capital One's storage space for which the ISRM-WAF-Role account had the requisite permissions.

15. Capital One tested the commands in the April 21 File, and confirmed that the commands did, in fact, function to obtain Capital One's credentials, to list or enumerate folders or buckets of data, and to extract data from certain of those folders or buckets. Capital One confirmed that the more-than-700 folders or buckets of data listed in the April 21 File matched the actual names of folders or buckets of data used by Capital One for data stored at Amazon. Capital One report that its computer logs reflect the fact that the List Buckets Command was in fact executed on April 21, 2019, and that the timestamp in Capital One's logs matches the timestamp in the April 21 File.

16. According to Capital One, its logs show a number of connections or attempted connections to Capital One's server from TOR exit nodes, and a number of connections from IP addresses beginning with 46.246, all of which Capital One believes relate to activity conducted by the same person involved in the April 21, 2019, intrusion, because they involve similar unusual communications through the misconfigured firewall to the server discussed above. Specifically, according to Capital One, the logs show:

- On or about March 12, 2019, IP address 46.246.35.99 attempted to access Capital One's data. I know, from checking publicly-available records, that this IP address is controlled by IPredator, a company that provides VPN services.
- On or about March 22, 2019, the ISRM-WAF-Role account was used to execute the List Buckets Command several times. These commands were executed from IP addresses that I believe to be TOR exit nodes. According

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to Capital One, the ISRM-WAF-Role account does not, in the ordinary course of business, invoke the List Buckets Command.

- Also on or about March 22, 2019, the ISRM-WAF-Role account was used to execute the Sync Command a number of times to obtain data from certain of Capital One's data folders or buckets. A number of those commands were executed from IP address 46.246.38.224. I know, from checking publicly-available records, that that IP address also is controlled by IPredator.
- One of the files copied from Capital One's folders or buckets on March 22, 2019, was a file with the name *****c000.snappy.parquet (the "Snappy Parquet File"), and this was the only time the ISRM-WAF-Role account accessed the Snappy Parquet File between January 1, 2019 and July 20, 2019.
- A List Buckets Command was executed on April 21, 2019, from IP address 46.246.35.103. I know, from checking publicly-available records, that the IP address from which this command was executed also is controlled by IPredator. I also believe, based on the timestamp on the April 21, 2019 file, and the time that Capital One reports that the command appears in Capital One's logs, that this was the command that was the source of the April 21 File.

17. According to Capital One, the data copied from Capital One's data folders or buckets includes primarily data related to credit card applications. Although some of the information in those applications (such as Social Security numbers) has been tokenized or encrypted, other information including applicants' names, addresses, dates of birth and information regarding their credit history has not been tokenized. According to Capital One, the data includes data regarding large numbers of applications, likely tens of millions of applications. According to Capital One, that data includes approximately 120,000 Social Security Numbers and approximately 77,000 bank account numbers.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. Capital One notified the Federal Bureau of Investigation of the data breach and provided additional information. As part of that referral, Capital One provided investigators with copies of internal logs, information and screenshots provided by the "white hat" tipster, and various screenshots of postings on the **SUBJECT ACCOUNTS**, including those described herein. I have reviewed that material provided by Capital One and, to the extent possible, independently viewed publicly accessible material and postings.

B. Evidence of Thompson's Involvement

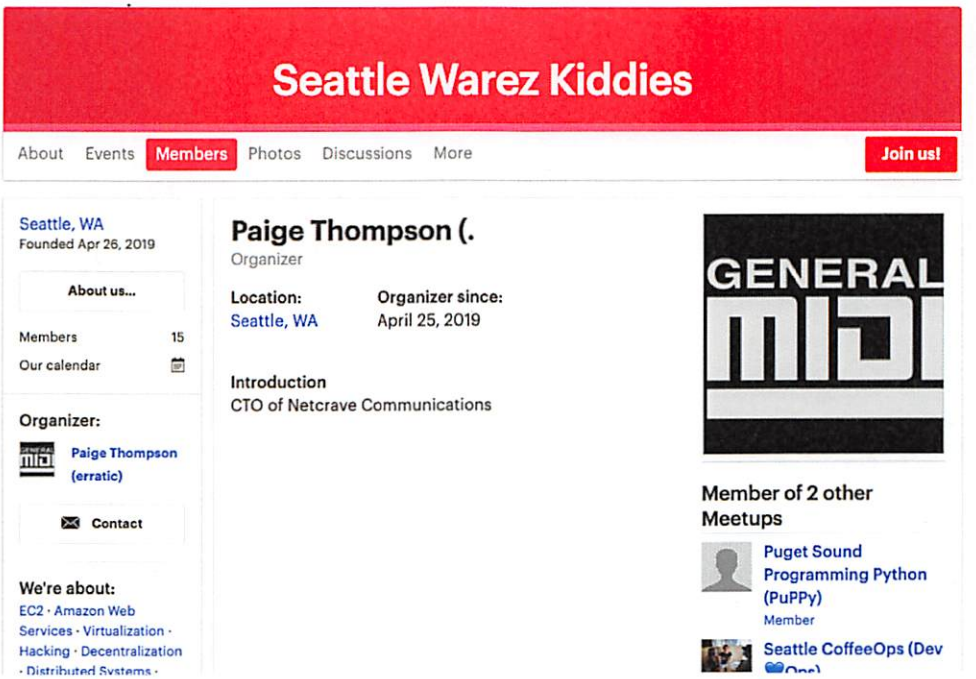
19. As noted above, the GitHub address for the April 21 File includes the name paigeadelethompson. Clicking on the name paigeadelethompson in the address takes the user to the main GitHub page for a Paige Adele Thompson, namely, **SUBJECT ACCOUNT 3**. The profile on that page contains a link to a GitLab page at www.gitlab.com/netcrave (the "GitLab Netcrave Page"). The GitLab Netcrave Page includes, among other things, a resume for a "Paige Thompson" of Seattle, Washington. That resume indicates that Thompson is a "systems engineer" and formerly worked at Amazon from May 2015- September 2016, specifically, with Simple Storage Services (commonly known as "S3). The resume also lists an address of 6520 28th Avenue South, Seattle, Washington, the address of the SUBJECT RESIDENCE. Based on this evidence, I believe that Thompson is the user of the GitHub and GitLab accounts described herein.

20. An April 19, 2019, post in the GitHub account of "pagieadelethompson" (**SUBJECT ACCOUNT 3**) includes a "Server List" of IP addresses associated with the account. All of the IP addresses in the Server List begin with 46.246. I have confirmed by checking publicly-available records that each of the IP addresses in the "Server List" is controlled by IPredator. (As noted above, Capital One reports that its logs reveal malicious activity, including malicious activity on April 19, 2019, that, similarly, comes from several IP addresses beginning with 46.246 that, based on publicly available records, are associated with the VPN service IPredator.)

21. Based on open source research, and based on information provided by Capital One, I am aware of a Meetup group called "Seattle Warez Kiddies" with a Web page located

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

at www.meetup.com\Seattle-Warez-Kiddies. That page indicates that its organizer is "Paige Thompson (erratic)" of Seattle, Washington.



Notably, the alias "erratic" matches the username of the Twitter account associated with Thompson, namely, **@0xA3A97B6C** (**SUBJECT ACCOUNT 1**).

22. On her Meetup group page, Thompson identified herself as the "CTO of Netcrave Communications." Moreover, on Thompson's GitLab Netcrave Page, Thompson lists herself as the owner of Netcrave Communications from 1999 to the present. Within Thompson's Meetup group is a link to the Slack channel **netcrave.slack.com** (the "Netcrave Slack Channel") (**SUBJECT ACCOUNT 2**), which I believe to be a Slack channel Thompson established and operated. The Netcrave Slack Channel was open and accessible to the public, meaning that any person could register for a Slack account and participate in the channels and chats and view the posts of other participants.

23. I have reviewed postings on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**), both those provided by Capital One and by viewing the channel itself. Among other things, on or about June 26, 2019, a user "erratic" posted a list of files that "erratic" claimed to possess. Among those files, two referenced "ISRM-WAF-Role." Based

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

on my review of the Sync Command in the April 21 File, and my training and experience, I know that the Sync Command would place extracted files in a directory with the name "ISRM-WAF-Role." Accordingly, I believe that, "erratic" was claiming to have files extracted using the extraction command set forth in the April 21 File.

24. On or about June 27, 2019, "erratic" posted on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**) about several companies, government entities, and educational institutions. Among these posts, "erratic" referred to "ISRM-WAF-Webrole" and indicated that account was associated with Capital One. Based on my training and experience, these communications appear to be references by "erratic" to other intrusions that "erratic" may have committed.

25. On or about June 27, 2019, another user posted "don't go to jail plz" on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**). In response, "erratic" posted "Im like > ipredator > tor > s3 on all this shit." I understand this to refer to the method Thompson used to commit the intrusion, namely, the use of IPredator (VPN) and TOR (among other things) to target S3 buckets stored on Amazon's cloud service . "[E]rratic" also posted "I wanna get it off my server that's why Im archiving all of it lol."

26. According to a screenshoot that Capital One provided, and that I have reviewed, on or about June 27, 2019, the user "paigeadele" posted on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**), "I've also got a leak proof IPredator router setup if anyone nneds [sic] it," as well as a GitHub link to **SUBJECT ACCOUNT 3** that included "paigeadelethompson" in the link. I was not able to locate this post on GitHub myself, although that may be because it since has been deleted.

27. According to a screenshot that Capital One provided, and that I have reviewed, on or about July 4, 2019, the user "paigeadele" posted on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**) a message seeking information about the Snappy Parquet File:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

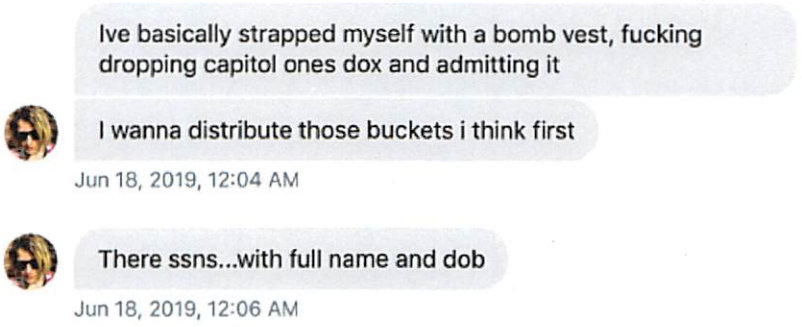
Notably, the Snappy Parquet File was one of the files exfiltrated from Capital One on March 22, 2019.

28. On or about July 19, 2019, the user "paigeadele" posted on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**) information about one of her pets. Included in the post was an estimate from a veterinarian dated June 10, 2019, provided to "Paige Thompson" at the address 6520 28th Avenue South, Seattle Washington, the address of the SUBJECT RESIDENCE. Based upon the information in the preceding paragraphs, I believe that Thompson is the person who posted under the names "erratic" and "paigeadele" on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**).

29. I have learned, from Capital One and through open-source research, of a Twitter account name **@0xA3A97B6C, with a username "ERRATIC" (SUBJECT ACCOUNT 1)**. I have reviewed photographs posted to the account of "ERRATIC," and they appear to depict the same individual who appears in photographs posted on the Netcrave Slack Channel (**SUBJECT ACCOUNT 2**) under the username "paigeadele. I believe that Thompson is the user of the "ERRATIC" Twitter account (**SUBJECT ACCOUNT 1**).

30. According to a screenshot that Capital One provided, on June 18, 2019, Twitter user "ERRATIC" sent a direct message on **SUBJECT ACCOUNT 1** to the reporting source: "Ive basically strapped myself with a bomb vest, fucking dropping capitol ones dox and admitting it. I wanna distribute those buckets i think first." Immediately thereafter, Twitter user "ERRATIC" followed with "There ssns…with full name and dob."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



I understand these posts to indicate, among other things, that Thompson intended to disseminate data stolen from victim entities, starting with Capital One, including private victim information such as names, dates of birth, and social security numbers.

31. As part of the investigation, investigators have viewed public activity of Twitter user "ERRATIC" (**SUBJECT ACCOUNT 1**) and observed various comments, including "tweets" and "retweets," that appear to relate to hacking and related data-access activity. For instance, on June 16, 2019, Twitter user "ERRATIC" posted the following about accessing instances, deploying a "backdoor," and copying ("mirror[ing]" S3 buckets):

32. I am aware that legal process directing production of subscriber records and information for the **SUBJECT ACCOUNTS** as well as other accounts believed to be associated with Thompson. As of the current date, to my knowledge, no responsive information or records have been received from the various providers.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. Search of the SUBJECT RESIDENCE

33. On July 26, 2019, I obtained a search warrant to search Thompson's residence, 6520 28th Avenue South, Seattle, Washington (the SUBJECT RESIDENCE), for evidence in this case. On July 29, 2019, other FBI Special Agents and I executed that search warrant. Five individuals, including Thompson, were present at the residence.

34. A search of a bedroom believed to belong to PAIGE A. THOMPSON resulted in the seizure of numerous digital devices. During the initial search of some of these devices, agents observed files and items that referenced Capital One and Amazon, other entities that may have been the targets of attempted or actual network intrusions, and "erratic," the alias associated with PAIGE A. THOMPSON.[1] Additionally, agents observed the Slack application installed on what is believed to be PAIGE A. THOMPSON's desktop computer. I also recognized Thompson from photographs posted on some of the **SUBJECT ACCOUNTS**, described above.

35. PAIGE A. THOMPSON was taken into custody and charged by criminal complaint with one count of Computer Fraud and Abuse, in violation of Title 18, United States Code, Section 1030(a)(2).

ADDITIONAL PROVIDER BACKGROUND

A. Twitter

36. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at http://www.twitter.com. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read character-limited messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

37. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20

[1] Based on items located in plain view during the search, the suspected owner and co-habitant of the SUBJECT RESIDENCE was arrested on unrelated charges.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

38. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

39. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" to their profile pages.

40. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

41. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 280 (formerly, 140) characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (i.e., a list of all "mentions" and "replies" for that username).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

42. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

43. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

44. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with http://t.co. This link service measures how many times a link has been clicked.

45. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitter users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

46. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

47. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

48. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

49. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

50. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

51. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

52. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculpate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

53. Therefore, the computers of Twitter are likely to contain the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

B. Slack

54. Slack is a cloud-based set of team-collaboration software tools and online services that can be accessed at http://www.slack.com. Slack allows users to establish "channels," in which a team can share messages, tools, and files. Slack offers many IRC-like features, including persistent chat rooms (channels) organized by topic, private groups, and direct messaging. Content, including files, conversations, and people, is all searchable

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

within Slack. Users can add emoji buttons to their messages, on which other users can then click to express their reactions to messages.

C. GitHub

55. GitHub is a company that provides webhosting and allows users to manage and store revisions of projects that can be accessed at http://www.github.com. It provides access control and several collaboration features such as bug tracking, feature requests, task management, and wikis for every project. Although used mostly for software development projects, GitHub also allows users to manage other types of files. GitHub is now owned by Microsoft Corporation.

56. Basically, GitHub is a place where programmers can store files that can be later accessed through the Internet. Programmers will often write code and upload it to GitHub where they can modify the code and update it via the Internet where it can be publicly available so programmers can collaborate. GitHub can also act as a place for programmers to publicly display their work. However, GitHub also offers private (and free) repositories.

57. GitHub offers plans for free, professional, and enterprise accounts. Free GitHub accounts are commonly used to host open source projects, such as by "users" and "collaborators." GitHub offers public and private repositories for accounts. According to its website, GitHub the following terminology:

- **Users** — Users are represented in our system as personal GitHub accounts. Each user has a personal profile, and can own multiple repositories. Users can create or be invited to join organizations or to collaborate on another user's repository.
- **Collaborators** — A collaborator is a user with read and write access to a repository who has been invited to contribute by the repository owner.
- **Organizations** — Organizations are a group of two or more users that typically mirror real-world organizations, such as businesses or projects. They are administered by users and can contain both repositories and teams of users.
- **Repositories** — A repository is one of the most basic GitHub elements. They may be easiest to imagine as a project's folder. A repository contains all of the project files (including documentation), and stores each file's revision history.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Repositories can have multiple collaborators and, at its administrators' discretion, may be publicly viewable or not.

- **Pages** — GitHub Pages are public webpages freely hosted by GitHub that users can easily publish through code stored in their repositories. If a user or organization has a GitHub Page, it can usually be found at a URL such as https://username.github.io or they may have the webpage mapped to their own custom domain name.
- **Gists** — Gists are snippets of source code or other text that users can use to store ideas or share with friends. Like regular GitHub repositories, Gists are created with Git, so they are automatically versioned, forkable and downloadable. Gists can either be public or secret (accessible only through a known URL). Public Gists cannot be converted into secret Gists.

58. On its website, GitHub offers a non-exhaustive list of the kinds of data GitHub maintains about users and projects on GitHub, namely:

- **Public account data** — There is a variety of information publicly available on GitHub about users and their repositories. User profiles can be found at a URL such as https://github.com/username. User profiles display information about when the user created their account as well their public activity on GitHub.com and social interactions. Public user profiles can also include additional information that a user may have chosen to share publicly. All user public profiles display:
    - Username
    - The repositories that the user has starred
    - The other GitHub users the user follows
    - The users that follow them

    Optionally, a user may also choose to share the following information publicly:

    - Their real name
    - An avatar
    - An affiliated company
    - Their location
    - A public email address
    - Their personal web page

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

- Organizations to which the user is a member (*depending on either the organizations' or the users' preferences*)

- **Private account data** — GitHub also collects and maintains certain private information about users as outlined in our Privacy Policy. This may include:
  - Private email addresses
  - Payment details
  - Security access logs
  - Data about interactions with private repositories

  To get a sense of the type of private account information that GitHub collects, you can visit your personal dashboard and browse through the sections in the left-hand menubar.

- **Organization account data** — Information about organizations, their administrative users and repositories is publicly available on GitHub. Organization profiles can be found at a URL such as https://github.com/organization. Public organization profiles can also include additional information that the owners have chosen to share publicly. All organization public profiles display:
  - The organization name
  - The repositories that the owners have starred
  - All GitHub users that are owners of the organization

  Optionally, administrative users may also choose to share the following information publicly:
  - An avatar
  - An affiliated company
  - Their location
  - Direct Members and Teams
  - Collaborators

- **Public repository data** — GitHub is home to millions of public, open-source software projects. You can browse almost any public repository (for example, the Atom Project) to get a sense for the information that GitHub collects and maintains about repositories. This can include:
  - The code itself
  - Previous versions of the code
  - Stable release versions of the project

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

- Information about collaborators, contributors and repository members
- Logs of Git operations such as commits, branching, pushing, pulling, forking and cloning
- Conversations related to Git operations such as comments on pull requests or commits
- Project documentation such as Issues and Wiki pages
- Statistics and graphs showing contributions to the project and the network of contributors

- **Private repository data** — GitHub collects and maintains the same type of data for private repositories that can be seen for public repositories, except only specifically invited users may access private repository data.
- **Other data** — Additionally, GitHub collects analytics data such as page visits and information occasionally volunteered by our users (such as communications with our support team, survey information and/or site registrations).

PRESERVATION REQUESTS

59. On or about July 22, 2019, the FBI sent preservation requests to the Providers requesting that they preserve all evidence related to the **SUBJECT ACCOUNTS.**

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

60. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit each Provider, and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to the Provider with direction that it identify the account(s) described in the corresponding Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachment B to this affidavit.

61. The search warrant will direct the Provider to create an exact copy of the specified account and records, including an exact copy of the contents of the hard disk drive or drives installed on the server associated with the pertinent **SUBJECT ACCOUNT(S)**, or the original drives.

62. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

63. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

CONCLUSION

64. Based on the forgoing, I request that the Court issue the proposed search warrants. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment Bs (attached

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

JOEL MARTINI
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN before me this 30 day of July, 2019.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Twitter Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data for the account associated with the following:

i. **@0xA3A97B6C, with username "ERRATIC"**

("**SUBJECT ACCOUNT**") as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Twitter, Inc., an electronic communications service and/or remote computer service provider headquartered at 1355 Market Street, Suite 900, San Francisco, California 94103.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

Items to be Seized

I. Information to be disclosed by Twitter, for search:

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Twitter, Inc. ("Twitter" or "Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

(a) All "Tweets" (message posts) and Direct Messages sent, received, "favorited," or retweeted by the account, including all photographs, video clips, or images included in those Tweets and Direct Messages, associated with the SUBJECT ACCOUNT from **August 1, 2017 to the present**;

(b) All identity and contact information, including full name, email address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(c) All past and current usernames, account passwords, and names associated with the account;

(d) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(e) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(f) All data and information associated with the profile page, including photographs, biographies ("bios"), and profile backgrounds and themes;

(g) All photographs and images in the user gallery for the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(h) All location data associated with the account, including all information collected by the "Tweet With Location" service and information regarding locations where the account was accessed;

(i) All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

(j) All data and information that has been deleted by the user;

(k) A list of all of the people that the user follows on Twitter (*i.e.*, the user's "following" list);

(l) A list of all users that the account has "unfollowed" or blocked;

(m) All "lists" created by the account, including friend or buddy lists;

(n) All information on the "Who to Follow" list for the account;

(o) All privacy and account settings;

(p) All records of Twitter searches performed by the account, including all past searches saved by the account;

(q) All information about connections between the account and third-party websites and applications;

(r) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least March 2019 to the present, including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking, intrusion, or network access activity; access to computers or servers of entities, including Capital One Financial Corporation ("Capital One"), or Amazon.com, Inc. or Amazon Web Services ("AWS") (collectively, "Amazon"), or to files, information, or data related to such entities; the possession, use, or transfer of authentication credentials or files, information, or data related to such entities, or otherwise related to stolen property;

(b) Evidence of the development, possession, or use of any code, scripts, or tools that could be used, whether along or in conjunction with other code, scripts, or tools, to search for or exploit vulnerabilities in networks or servers;

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking, cloud storage (e.g., AWS, Azure, Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(h) Any address lists or buddy/contact lists associated with the specified account;

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code, described above.

(j) All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Slack Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data for the account associated with the following:

i. **netcrave.slack.com**

("SUBJECT ACCOUNT") as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Slack Technologies, an electronic communications service and/or remote computer service provider headquartered at 500 Howard Street, San Francisco, California 94105.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

Items to be Seized

I. Information to be disclosed by Slack, for search:

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Slack Technologies ("Slack" or "Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

(a) All chat communications (channels), including all attachments, files, photographs, video clips, or images included or attached to such communications, associated with the SUBJECT ACCOUNT from August 1, 2017 to the present;

(b) All other communications, including Direct Messages sent, received, "favorited," including all attachments, files, photographs, video clips, or images included or attached to such communications, involving user "erratic" or "paigeadele" from August 1, 2017 to the present;

(c) All communications, including, but not limited, to chat rooms (channels) and Direct Messages sent, received, "favorited," including all attachments, files, photographs, video clips, or images included or attached to such communications, associated with the SUBJECT ACCOUNT from **August 1, 2017 to the present**;

(a) All identity and contact information, including full name, email address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames, account passwords, and names associated with the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(e) All data and information associated with the profile page, including photographs, biographies ("bios"), and profile backgrounds and themes;

(f) All photographs and images for the account;

(g) All location data associated with the account, including all information regarding locations where the account was accessed;

(h) All data and information that has been deleted by the user;

(i) All "lists" created by the account, including friend or buddy lists;

(j) All privacy and account settings;

(k) All records of searches performed by the account, including all past searches saved by the account;

(l) All information about connections between the account and third-party websites and applications;

(m) All records pertaining to communications between Provider and any person regarding the user or the user's account, including contacts with support services, and all records of actions taken, including suspensions of the account.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least March 2019 to the present, including, for each account or identifier listed on Attachment A-2, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking, intrusion, or network access activity; access to computers or servers of entities, including Capital One Financial Corporation ("Capital One"), or Amazon.com, Inc. or Amazon Web Services ("AWS") (collectively, "Amazon"), or to files, information, or data related to such entities; the possession, use, or transfer of authentication credentials or files, information, or data related to such entities, or otherwise related to stolen property;

(b) Evidence of the development, possession, or use of any code, scripts, or tools that could be used, whether along or in conjunction with other code, scripts, or tools, to search for or exploit vulnerabilities in networks or servers;

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking, cloud storage (e.g., AWS, Azure, Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

(h) Any address lists or buddy/contact lists associated with the specified account;

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

described above.

(j) All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-3

GitHub Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data for the account associated with the following:

i. **https://gist.github.com/paigeadelethompson/**

("SUBJECT ACCOUNT") as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by GitHub, Inc., an electronic communications service and/or remote computer service provider headquartered at 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California 95833.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-3

Items to be Seized

I. Information to be disclosed by GitHub, for search:

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of GitHub, Inc. ("GitHub" or "Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

(d) All content, including, but not limited to, communications, posts, pages, gists, repositories (whether private, public, or organization), and files associated with the SUBJECT ACCOUNT;

(e) All account and profile data (whether private, public, or organization) associated with the account and the information, both current and preserved, associated therewise, including username, repositories that the user has starred, other GitHub users the user follows, users that follow them, real name, avatar, affiliated company, location, email address, personal web page, payment details, security access logs, page visits;

(f) For each gist or repositiory for the account, a list of all "users" and "collaborators";

(g) All identity and contact information, including full name, email address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(h) All past and current usernames, account passwords, and names associated with the account;

(i) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(j) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(k) All data and information associated with the profile page, including photographs, biographies ("bios"), and profile backgrounds and themes;

(l) All photographs and images for the account;

(m) All location data associated with the account, including all information regarding locations where the account was accessed;

(n) All data and information that has been deleted by the user;

(o) All "lists" created by the account, including friend or buddy lists;

(p) All privacy and account settings;

(q) All records of searches performed by the account, including all past searches saved by the account;

(r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Provider and any person regarding the user or the user's account, including contacts with support services, and all records of actions taken, including suspensions of the account.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least March 2019 to the present, including, for each account or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

identifier listed on Attachment A-3, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking, intrusion, or network access activity; access to computers or servers of entities, including Capital One Financial Corporation ("Capital One"), or Amazon.com, Inc. or Amazon Web Services ("AWS") (collectively, "Amazon"), or to files, information, or data related to such entities; the possession, use, or transfer of authentication credentials or files, information, or data related to such entities, or otherwise related to stolen property;

(b) Evidence of the development, possession, or use of any code, scripts, or tools that could be used, whether along or in conjunction with other code, scripts, or tools, to search for or exploit vulnerabilities in networks or servers;

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking, cloud storage (e.g., AWS, Azure, Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

(h) Any address lists or buddy/contact lists associated with the specified account;

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code, described above.

(j) All subscriber records associated with the specified account, including name,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970